REMARKS

The present application was filed on June 20, 2003 with claims 1-16. Claims 1, 8, 9 and 16 are the independent claims.

In the new non-final Office Action, the Examiner: (i) maintains the rejection of claims 1, 2, 4-6, 8-10, 12-14 and 16 under 35 U.S.C.§103(a) as being unpatentable over U.S. Patent No. 6,697,488 (hereinafter "Cramer") in view of U.S. Patent No. 5, 515, 441 (hereinafter "Faucher"); and (ii) maintains the rejection of claims 3, 7, 11 and 15 under 35 U.S.C.§103(a) as being unpatentable over Cramer and Faucher in view of a Cramer et al. article entitled "Multiparty Computation from Threshold Homomorphic Encryption" (hereinafter "Cramer paper").

Applicant believes that the present claims are patentably distinct over Cramer, Faucher, and the Cramer paper, alone and/or in combination. Applicant thus respectfully traverses the outstanding rejections, and requests reconsideration of the present application in view of the remarks below.

Currently amended claim 1 is directed to a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of: obtaining the ciphertext in the first party device sent from a device associated with a second party; and generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but such that neither can decrypt the ciphertext alone. Independent claims 8, 9 and 16 have been amended in a similar manner.

With regard to the §103(a) rejections, each and every limitation of the independent claims is not met by the collective teachings of Cramer and Faucher. Below, Applicant explains how such portions of Cramer and Faucher fail to teach or suggest each and every limitation. While Applicant

may refer from time to time to each reference alone in describing its deficiencies, it is to be understood that such arguments are intended to point out the overall deficiency of the cited combination.

The present Office Action asserts that the previous clarifying limitation added by Applicant in their last response, i.e., "the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds," is disclosed by Faucher at column 8, lines 8-55 and Fig. 5. Applicant strongly disagrees with this assertion.

It is to be understood that the claimed invention provides for a jointly performed decryption operation of a given ciphertext. That is, as made clear by the claim language, the first party and the second party each perform one or more subcomputations of the singular decryption operation that results in the decryption of the given ciphertext, and that such subcomputations are based at least in part respective partial shares of a key that each party holds. Thus, neither party can decrypt the given ciphertext alone.

Faucher discloses a completely different protocol. As column 8 and Fig. 5 of Faucher clearly illustrate, while two terminals cooperate in a cryptographic type protocol, the Faucher protocol is a key exchange and not a decryption operation. Also, while there is information exchanged between the two Faucher terminals and decryptions are performed, no where do the two Faucher terminals "jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds," as recited in the independent claims. In fact, the entire protocol of column 8 of Faucher is performed in order to generate a session key, which is done by each terminal performing separate decryption operations of certificates received from the other terminal. There is no joint performance of a joint decryption operation whereby each terminal performs subcomputations of the joint decryption operation. Nor is there any disclosure in Faucher that suggests that any such subcomputations are based at least in part respective partial shares of a

key that each party holds. In fact, column 8 of Faucher confirms this deficiency by clearly explaining that each terminal decrypts the other's certificate using the KCA public decryption key.

The present Office Action further points to column 2, lines 14-20 of Faucher to assert that here Faucher discloses that the session key that is generated between the first and second parties is used to "decrypt the ciphertext." However, column 2, lines 14-20 of Faucher says no such thing. What is stated there is that the session key agreement protocol of Faucher is capable of preventing the "man-in-the-middle-attack." This is done in the manner disclosed at columns 7 and 8 of Faucher by requiring an authentication process between the first and second parties based on the session key, see column 7, lines 2-23. Since the "man-in-the-middle" cannot generate the session key, he cannot spoof the authentication process between the first and second parties.

Again, Faucher clearly does not disclose that the first party and the second party each perform one or more subcomputations of the singular decryption operation that results in the decryption of the given ciphertext, and that such subcomputations are based at least in part respective partial shares of a key that each party holds. The operations between the first and second parties in Faucher are performed to generate a session key so that each party can be authenticated to the other for any subsequent transfers, not to jointly decrypt the ciphertext.

Cramer fails to remedy theses deficiencies of Faucher. Accordingly, it is believed that the combined teachings of Cramer and Faucher fail to meet the limitations of claim 1.

Also, Applicant maintains that the Examiner has failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed. Applicant respectfully submits that the conclusory statements made in the final Office Action to support motivation to combine Cramer and Faucher are of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14 (U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to combine Cramer and Faucher to produce the particular limitations in question. The statements of

motivation provided by the Examiner appear to be conclusory statements of the type ruled insufficient in KSR v. Teleflex.

For at least these reasons, Applicant asserts that claim 1 is patentable over Cramer and Faucher.

Currently amended independent claim 9 includes limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1.

Currently amended claims 8 and 16, which recite limitations from the perspective of the other device, and include limitations similar to those of claim 1, are therefore believed allowable for reasons similar to those described above with reference to claim 1. For at least these reasons, Applicant asserts that claims 8 and 16 are patentable over Cramer and Faucher.

Dependent claims 2, 4-6, 10 and 12-14 are allowable for at least the reasons identified above with regard to claims 1 and 9. One or more of these claims are also believed to define separately-patentable subject matter over the cited art.

Claims 2 and 10 recite an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation. The Examiner refers to Cramer at column 7, lines 1-40 and column 9, lines 25-45 as teaching or suggesting the limitations of claims 2 and 10. Although Cramer at column 7, lines 25-26 refers to a public key represented by the numbers g_1, g_2, c, d, and h, the relied-upon portions of Cramer do not teach or suggest an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party cannot read the information but can use the information to perform an operation.

Claims 4 and 12 recite generating a share of a random secret; generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; transmitting at least the encrypted information to the second party device; and computing the

plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device. The Examiner refers to Cramer at column 7, lines 11-19 as teaching or suggesting the step of generating a share of a random secret. The relied-upon portion of Cramer refers to a private-key choosing step, and does not teach or suggest generating a share of a random secret. Although Cramer, at column 7, lines 10-27 refers to private key Z_q, the relied-upon portions of Cramer do not teach or suggest generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext. Furthermore, although Cramer at column 9, lines 25-50 refers to recovering the plaintext m in the decryption step 50, Cramer does not teach or suggest computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

With regard to claims 5 and 13, the relied-upon portions of Cramer do not teach or suggest the recited limitation. Column 7, lines 10-15 of Cramer refers to private-key choosing step 13, and column 9, lines 35-40 refer to decryption of an encryption of a message, which do not teach or suggest the first party device and the second party device additively share components of a private key.

With regard to claims 6 and 14, Cramer at column 8, line 38 through column 9, line 23 refers to verification of ciphertext 30 in verification step 40. Although the relied-upon portion of Cramer refers to verifying ciphertext 30, the relied-upon portion of Cramer does not teach or suggest generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

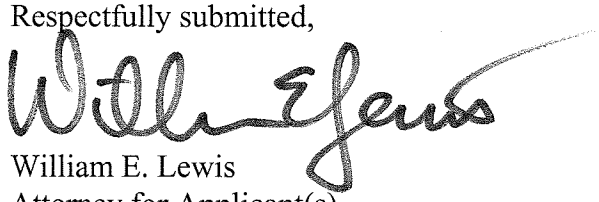
Accordingly, withdrawal of the §103(a) rejection of claims 1, 2, 4-6, 8-10 12-14 and 16 is respectfully requested.

With regard to the rejection of claims 3, 7, 11 and 15 as being unpatentable over Cramer and Faucher in view of Cramer paper, Applicant asserts that the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer and Faucher. Thus, claims 3, 7, 11 and 15 are patentable at least by virtue of their dependency from claims 1 and 9. Claims 3, 7, 11 and 15 also recite patentable subject matter in their own right.

Accordingly, withdrawal of the §103(a) rejection of claims 3, 7, 11 and 15 is respectfully requested.

In view of the above, Applicant believes that claims 1-16 are in condition for allowance, and respectfully requests withdrawal of the various §103(a) rejections.

Respectfully submitted,



Date: March 9, 2009

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946